Double-Lock or Double-Bind? The Investigatory Powers Bill and Freedom of Expression in the United Kingdom

'Double Bind'

> A situation in which a person is confronted with two irreconcilable demands or a choice between two undesirable courses of action.
>
> (Oxford Dictionary)

Introduction/background

The Snowden revelations, uncovering the scale of surveillance by amongst others, the National Security Agency (NSA) in the United States of America and Government Communications Headquarters (GCHQ) in the United Kingdom, continue to reverberate.[1] From then (summer 2013) until now, it can be safely said that international terrorism and its use of modern technology to both plan and execute guerrilla style atrocities such as the recent attacks in Turkey, France and Belgium [2] have changed at a dizzying pace the world in which we live and the context within which governments have to attempt to ensure basic safety for citizens. Against this background national and international attempts to reconcile rapidly evolving mass surveillance capabilities with upholding notions of the rule of law have proven very difficult. The United Kingdom is no exception. The Investigatory Powers Bill (the IP Bill)[3] currently being considered by Parliament and set to be enacted and in force by the end of 2016 is highly controversial.

As with all new legislation in the UK, section 19 of the Human Rights Act 1998 requires the Minister in charge of a Bill to make a statement as to whether or not it is compatible with Convention[4] rights. The Home Office duly published a short document in March 2016 noting that the IP Bill engages three rights, and extensively dealt with the Bill's foreseeable impact on the Article 8 right to privacy.[5] Although it admits that the Bill also engages Article 10, the right to freedom of expression, notably less attention is given to both the Bill's impact on this right and the way in which it proposes to deal

[1] For a concise, interactive synopsis of the impact of surveillance culture, the Snowden leak and the virtual impossibility of avoiding surveillance in modern society, *see* Rory Cellan-Jones, *Who's Watching Me on the Internet?, BBC iWonder* (2016) available at http://www.bbc.co.uk/guides/zyvmhv4, accessed 21 May 2016.

[2] See Jon Henley and Kareem Shaheen , *Suicide bombers in Brussels had known links to Paris attacks, The Guardian*, (March 23, 2016).

[3] The Investigatory Powers Bill 2015, HC Bill 143, perhaps tellingly commonly referred to in the media as 'the Snooper's Charter'. *See* Rowena Mason, Anushka Asthana and Alan Travis, *'Snooper's charter': Theresa May faces calls to improve bill to protect privacy, The Guardian*, (March 15, 2016), accessed April 27,2016.

[4] European Convention of Human Rights.

[5] HOME OFFICE, INVESTIGATORY POWERS BILL – EUROPEAN CONVENTION ON HUMAN RIGHTS MEMORANDUM, (March 8, 2016), available at https://www.gov.uk/government/publications/investigatory-powers-bill-overarching-documents (last accessed May 11,2016).

with such impact. Similarly campaigners opposing the Bill have mostly rallied around raising privacy concerns.[6]

It is submitted that not according freedom of expression at least equal weight in this debate is unfortunate to say the least, and at most a risky oversight, especially when one considers that very recently a major area of the English common law was completely overhauled because of freedom of expression concerns with the enactment and coming into force of the Defamation Act 2013.

This essay therefore puts aside, for the time being, the privacy concerns raised by the IP Bill, and instead focuses on its implications for freedom of expression. How then, to go about judging the Bill? A useful framework to follow may be a simple Burkean analysis: Any proposed change in laws needs to start by showing, first, that there's a need for change; second, that the proposed change will solve the problem it claims to solve; and third, that the benefits of the change will outweigh its costs.[7] The following discussion proceeds broadly along these lines, with the first section examining the current state of play in the UK regarding data surveillance and its regulatory framework, the second section taking a closer look at the IP Bill and the third section analysing its likely impact against freedom of expression in the UK. Given the length and range of the Bill, the discussion focuses on metadata and bulk surveillance.

1. The problem

1.1 Current surveillance in the UK

Residents and visitors to the UK find themselves subject to some of the most intrusive and extensive surveillance regimes in the world. In fact, it is no exaggeration to say that the Snowden leaks showed that the extent to which the inhabitants of the United Kingdom is already subject to surveillance is truly staggering. Not only are surveillance cameras ubiquitous,[8] the UK also boasts one of the largest DNA databases in the world,[9] and the Don't Spy On Us (DSOU)[10] campaign group highlighted that

---

[6] The third right that is engaged is the right to protection of property contained in Article 1 of the First Protocol of the Convention.

[7] EDMUND BURKE, REFLECTIONS ON THE REVOLUTION IN FRANCE, WORKS OF EDMUND BURKE, VOLUME 3 OF 12, Kindle Edition 2016. It is submitted that the pragmatism with which Burke sets about relating abstract notions to real life is very useful, especially in the common law. Therefore, at the risk of oversimplifying, Burkean conservatism in the sense used in this essay simply means the application of the precautionary principle to the legislative sphere.

[8] There are estimated to be more than 6 million CCTV cameras active in the UK, with more than 100 000 publicly operated cameras under the supervision of the Office for Surveillance Commissioners. Matthew Weaver interview with Tony Porter, *UK public must wake up to risks of CCTV, says surveillance commissioner, The Guardian,* (January 6 2015).

[9] The DNA database currently holds details of some 5,156,268 individuals - HOME OFFICE, NATIONAL DNA DATABASE STATISTICS, Q4 2015 TO 2016, available at https://www.gov.uk/government/statistics/national-dna-database-statistics, (last accessed May 11, 2016).

[10] The Don't Spy On Us (DSOU) campaign is a coalition of organisations that defend privacy, freedom of expression and digital rights, and the members of its executive committee are ARTICLE 19, Big Brother Watch, English PEN, Liberty, Open Rights Group and Privacy International. *See* DON'T SPY ON US, REFORMING SURVEILLANCE IN THE UK, (September 2014), Joint publication by ARTICLE 19, Big Brother Watch, English PEN, Liberty, Open Rights Group and Privacy International, available at <https://www.dontspyonus.org.uk/blog/2014/09/19/reforming-surveillance-we-publish-our-policy-paper/ > accessed 11 May 2016, p 1.

GCHQ through its 'TEMPORA' programme was routinely and daily intercepting private communications of millions of British residents to the scale of 21 petabytes of data. To put it in context, this translates to the equivalent of downloading the entire British Library 192 times *per day*.[11] The latter large-scale interception enabled GCHQ to construct a huge database of communications data, or metadata. This is significant because the technology on metadata enables the construction of a clear picture about individuals, without having to directly analyse the *content* of their communications. So while significant procedural and other safeguards were in place regarding the monitoring of individual, targeted communications, the position around metadata and bulk communications data was largely without regulation and therefore exploitable, as will become clear below.

1.1.1 Direct surveillance not needed for picture to emerge

When the IP Bill's predecessor[12] was debated in early 2000, only a quarter of the UK population was online, whereas now more than 80 per cent are, with the average household owning several internet enabled devices.[13] These devices routinely track details of websites their users visit, their location, who they chat to or text, etc. People's smartphones not only store telephone numbers and addresses, but also personal information about their finances, family members, religious and political views, medical history and so on. With current technology it is possible to use this information to build up comprehensive pictures of individual lives without the need to listen to calls or read emails.[14] Stewart Baker, ex-NSA General Counsel, said, "…metadata absolutely tells you everything about somebody's life. If you have enough metadata, you don't really need content."[15] More chillingly, the former director of the NSA and the CIA, General Michael Hayden, asserted, "We kill people based on metadata."[16]

It is against this background that reassuring statements from the Office of Surveillance Commissioners (the OSC) need to be read: If one examines the latest report by the OSC, the level of *direct* surveillance in the UK seem reasonable and subject to rigorous oversight. Indeed, the report shows a *decrease* in instances of authorised surveillance. [17] The OSC therefore felt confident enough to reassure the public that its annual statistics show that all such activity that they oversee is accounted for, properly authorised according to set procedures and once undertaken, overseen until cancelled. It went on to point out that the number of authorisations for these types of covert activity is far less than is sometimes portrayed – but tellingly, it then stated that the seeming 'over-portrayal of surveillance' seems to come from those,"… who continue to confuse these activities with the access to communications data powers (Part 1 of RIPA").[18] As seen above, directed surveillance is not necessary for a complete picture to emerge or for an individual to be accurately

---

[11] DSOU p 4.

[12] THE REGULATION OF INVESTIGATORY POWERS ACT 2000 ('RIPA').

[13] *See* for up to date statistics on internet use in the UK the OFCOM website at http://media.ofcom.org.uk/facts/.

[14] DSOU, 16.

[15] David Cole, *We Kill People Based on Metadata, New York Review of Books* (May 10, 2014).

[16] Ibid.

[17] OSC REPORT 2014/2015 p 11-15 dealing with property interference, intrusive surveillance, directed surveillance, and covert human intelligence sources.

[18] OSC REPORT 2014/2015 p 30 para 5.51.

profiled – access to metadata is enough. It is precisely this aspect which the IP Bill proposes to place on a legal footing and which is the subject of this discussion.

1.2 Current legal landscape

Several key statutes and cases need to be mentioned to place the IP Bill in context. These include the Regulation of Investigatory Powers Act 2000, the EU's Data Retention Directive and the case (*Digital Rights Ireland*) which made short shrift of it, and the UK's response to this in the form of the Data Retention and Investigatory Powers Act 2014. The latter, in turn, was deemed to be not fit for purpose in the UK's "Davis case",[19] with a reference to the CJEU currently under way.[20]

1.2.1 RIPA – the Regulation of Investigatory Powers Act 2000

This Act, which is still in place and therefore forms the bulk of the regulatory framework within which surveillance takes place in the UK, was envisaged to ensure that relevant investigatory powers, including the interception of communications, acquisition of communications data, intrusive and covert surveillance and access to encrypted data are used in accordance with human rights.[21] It has been more than fifteen years since its inception now, which timespan has witnessed the massive expansion of surveillance powers and data analysis capabilities, combined with the rise of social media and advances in communications technology. It is safe to say that nobody still thinks that this Act and the regulatory framework it oversees is fit for purpose – developments have outpaced the law to such an extent that the massive surveillance operations uncovered by the Snowden revelations were by and large legal in the sense that no law was actually breached, mainly because the law itself did not envisage the type of data analysis made possible by technological advances. The following example from the operation of this Act suffices to illustrate the kind of loopholes meant in this discussion.

The Act is relatively robust in providing checks and balances for targeted interception in the sense of interception of communications by and to identified persons, but (much) less so when this is not the main route or rationale for the interception. For example, there are strenuous conditions[22] attached to the issuance of an interception warrant in terms of section 8(1)(a) where a single person can be named or identified as the interception subject – but section 8(4) read with (5) largely removes these safeguards if the interception relates to 'external communications', for which a lesser warrant is obtained. In this way, section 8(4) warrants could be (and were, per the Snowden revelations) used as the basis for mass interception by GCHQ of bulk communications data.[23] The Government admitted in May 2014 that it understood 'external communications' to include, for example, social media such as Facebook – so long as the relevant server was outside the UK.[24] In fact, many internal

[19] R. (on the application of Davis) v Secretary of State for the Home Department, EWHC 2092 (Admin) [2015].

[20] C-698/15 - *Davis and Others*.

[21] REGULATION OF INVESTIGATORY POWERS ACT 2000, Explanatory Notes, p 1 par. 3.

[22] Such as the requirement in s. 8(2) that the warrant must comprise one or more schedules setting out the addresses, numbers, apparatus or other factors that are to be used for identifying the communications that may be or are to be intercepted, and the targeted nature of such interception is further developed in s. 8(3) where it is required that this must be limited to communications that are likely to include communications intended to or from the named person.

[23] DSOU, 11.

[24] Charles Blandford Farr, Director General of the Office for Security and Counter-Terrorism, Witness Statement for the Respondents in *Privacy International and others against the Secretary of State, GCHQ and*

messages and most cloud based communications are routed via other countries, and would thus fall within this understanding of 'external communications'. In addition, regardless of whether communications are internal or external, the Act places no restrictions on the collection of communications data by GCHQ.[25] The result is this: searches directly referencing identified persons (e.g. with the search term 'Jane Doe') are not allowed or at least very difficult to warrant, whereas searches on the basis of other terms are, as long as the search showed some facet of 'external communications' or comprised bulk communications data – and in this way even though 'Jane Doe' may never have been directly named or searched, a comprehensive picture of her could nevertheless still be formed by analysing such bulk data.

A further loophole exists in the distinction between 'communications', which are strongly protected, and 'communications data', which is not.[26] In the light of current data analysis capabilities, this distinction is arbitrary and useless.

1.2.2 Data Retention Directive

Here the focus needs to shift to the European Union's Data Retention Directive,[27] which mandated EU States' retention of communications data on their entire populations for up to a year in order to combat crime by, inter alia, requiring telephone communications service providers to retain traffic and location data.

1.2.3 Digital Rights Ireland case[28]

The European Court of Justice was asked for a preliminary ruling on the validity of the Directive. The Court held that EU-mandated mass surveillance "entails an interference with the fundamental rights of practically the entire European population"[29] and that the interference was not limited to what was strictly necessary.[30] The blanket retention of communications data as well as the lack of independent judicial decision making about access to data was found to be disproportionate.[31] The CJEU therefore declared the Data Retention Directive not compatible with the Charter of Fundamental Rights of the European Union Article 7 (the right to respect for family and private life) and Article 8 (the right to protection of personal data).

---

others, cases IPT/13/92/CH; IPT/1377/H; IPT/13/204/CH; IPT/13/168-173/H; IPT/13/204/CH (May 16,2014), para 137 and para 138 where the same is repeated for Twitter.

[25] Section 16(2) provides: "…intercepted material falls within this subsection so far only as it is selected to be read, looked at or listened to otherwise than according to a factor which – (a) is referable to an individual who is known to be for the time being in the British Islands; and (b) has as its purpose, or one of its purposes, the identification of material contained in communications sent by him, or is intended for him." In other words, only targeted communication falls under the safeguards of ss. 15 and 16 provided in RIPA.

[26] For example, Part 1 of RIPA dealing with the interception of 'communications' require a warrant from the Secretary of State, whereas access to communications data under Part 2 requires only authorisation by a senior member of the relevant public body.

[27] DIRECTIVE 2006/24 ON THE RETENTION OF DATA GENERATED OR PROCESSED IN CONNECTION WITH THE PROVISION OF PUBLICLY AVAILABLE ELECTRONIC COMMUNICATIONS SERVICES OR OF PUBLIC COMMUNICATIONS NETWORKS.

[28] *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and others* (Joined Cases C-293/12, C-594/12), EU:C:2013:845, EU:C:2014:238, [2015] Q.B. 127.

[29] *Id.*, at para 56.

[30] *Id.*, at para 65.

[31] *Id.*, at paras 59 and 62.

1.2.2 DRIPA

In response to the Data Retention Directive, the UK fast-tracked emergency legislation in the form of the Data Retention and Investigatory Powers Act 2014 (DRIPA), only for the Act to be declared "inconsistent with European Union Law" shortly after the decision in *Digital Rights Ireland*:

Davis case

In a judicial review jointly pursued by Messrs Davis and Watson (Conservative and Labour Members of Parliament respectively) against the Secretary of State,[32] the high court held DRIPA incompatible with European Union Law as set out in *Digital Rights Ireland*, on the grounds that section 1 of DRIPA is incompatible with Articles 7 and 8 of the Charter of Fundamental Rights, to the extent that it does not restrict the purposes for which communications data may be accessed to serious crime, and access to the data is not made dependent on a prior review by a court or an independent administrative body whose decision limits access to and use of the data to what is strictly necessary for the purpose of attaining the objective pursued.[33]

Rulings by the European Court of Justice (CJEU) in Luxembourg relate to EU regulations and are binding on British courts, although the Home Secretary appealed the *Davis* decision arguing that such decisions are not mandatory as far as domestic legislation is concerned. The Court of Appeal agreed - at the end of 2015 it provisionally set out its disagreement with the Divisional Court's finding above.[34] In a preliminary ruling which raises fundamental issues regarding the relationship between English domestic legislation and European Union law, the Appeal Court expressed the provisional view that the judgment of the Court of Justice in *Digital Rights Ireland* did not lay down, in relation to retained communications data, mandatory requirements of EU law with which national legislation had to comply.[35] The Home Office interprets this as meaning that the CJEU was only concerned with the legality of the EU legislation, and that therefore its findings should not be applied to domestic legislation. The government also argues that domestic access regimes should not be read as implementing EU law (and as such should not be subject to EU Law and the Charter).[36] This, it is submitted, is disingenuous given that DRIPA was clearly enacted for the very reason of implementing EU law in the UK.[37]

The Court of Appeal has referred questions as to the interpretation of the *Digital Rights Ireland* case to the CJEU (C-698/15 - Davis and Others). At present, a ruling is due in this case together with another preliminary reference from Sweden (Tele2).

Whatever the outcome of the CJEU referral and notwithstanding the UK's decision to leave the European Union as per the referendum result of 24 June 2016, DRIPA is subject to a sunset clause of 31 December 2016, so new legislation will have to be enacted.

---

[32] *R. (on the application of Davis) v Secretary of State for the Home Department*, [2015] EWHC 2092 (Admin).

[33] *Id.*, at 114.

[34] *Davis and others* EWCA Civ 1185**.**

[35] *Id.,* at H2.

[36] HOME OFFICE *op. cit,.* para 111, where the Home Office also goes on to say: "Safeguards in domestic access regimes should be a matter or the domestic courts. The requirements of the Charter do not in any event go beyond the requirements of Article 8, and the provisions of DRIPA are compatible with the Convention."

[37] At the time of submitting this article, the United Kingdom have just voted to leave the European Union, further complicating for the foreseeable future the status of EU law and of pronouncements by the CJEU.

Summing up: Surveillance and in particular the interception, monitoring and analysis of bulk communications data, takes place against a very fragmented legal background. It is questionable whether existing legislation properly addresses this issue in itself, and to the extent that it does, it is unclear as to whether Convention and Charter rights are adequately addressed. Everyone agrees that this situation needs to be addressed.[38] It is against this background that we turn to the Bill at issue.

2. The Proposed Solution : The Investigatory Powers Bill 2015 (HC Bill 143)

2.1 Overview

The Investigatory Powers Bill (IP Bill) was announced in the Queen's Speech on 27 May 2015[39] and introduced to the House of Commons on 1 March 2016 after its predecessor the Draft Communications Data Bill[40] were dealt a death blow by the government's then coalition partners. It aims to provide a new framework to govern the use and oversight of investigatory powers by law enforcement and the security and intelligence services, mainly by changing the existing law relating to the use and oversight of these powers. As already mentioned, the new legislation needs to be in force by 31 December 2016,[41] mainly because DRIPA is subject to a sunset clause by this date. According to the UK Government, the proposed legislation does the following three things:

> 1. "It brings together all of the powers already available to law enforcement and the security and intelligence agencies to obtain communications and data about communications. It will make these powers and the safeguards that apply to them clear and understandable.
> 2. It radically overhauls the way these powers are authorised and overseen. It introduces a 'double-lock' for interception warrants, so that, following Secretary of State authorisation, these (and other warrants) cannot come into force until they have been approved by a judge. And it creates a powerful new Investigatory Powers Commissioner to oversee how these powers are used.
> 3. It ensures powers are fit for the digital age. The bill makes provision for the retention of internet connection records for law enforcement to identify the communications service to which a device has connected. This will restore capabilities that have been lost as a result of changes in the way people communicate."[42]

The Bill itself is certainly long and complex – it comprises 233 sections split in nine parts with a further ten schedules, spanning some 260 pages (the annotated version spans 701 pages). To this should be added six draft codes of practice setting out how powers and obligations will work in

---

[38] *See* the comprehensive review of investigatory powers legislation commissioned by Parliament: DAVID ANDERSON QC, *A QUESTION OF TRUST: REPORT OF THE INVESTIGATORY POWERS REVIEW*, (June 2015).

[39] HANSARD, HOUSE OF COMMONS Vol.596 col.32 (May 27, 2015).

40 (London, 2012), Cm.8359.

[41] HOME OFFICE, INVESTIGATORY POWERS BILL, Published March 1, 2016, updated March 4, 2016, available at https://www.gov.uk/government/collections/investigatory-powers-bill (last accessed May 9, 2016).

[42] The Chapeau to the Bill reads as follows: "Make provision about the interception of communications, equipment interference and the acquisition and retention of communications data, bulk personal datasets and other information; to make provision about the treatment of material held as a result of such interception, equipment interference or acquisition or retention; to establish the Investigatory Powers Commissioner and other Judicial Commissioners and make provision about them and other oversight arrangements."

practice, adding a further 409 pages of legislation to an already bulky proposed statute.[43] The Bill engages the European Convention on Human Rights (ECHR), in particular Article 8 (right to respect for private and family life), Article 10 (freedom of expression) and Article 1 of the First Protocol of the Convention (protection of property).

The proposed legislation has so far been met with ambivalence, to say the least: After largely incorporating comments by the House of Commons Science and Technology Committee, the Intelligence and Security Committee of Parliament and a Joint Committee of both Houses of Parliament, the IP Bill passed its second reading in the House of Commons on 15 March 2016 with 281 votes for and just 15 against,[44] but this must be placed in context: The Labour party (the official opposition) and the Scottish National Party (SNP) abstained from voting, indicating unease with the Bill without at this stage completely blocking its progress through Parliament. What is more, almost 50 Conservative MPs were absent, which may indicate that a large faction in the ruling party may not be satisfied with the Bill as it currently stands.

So, which features of this comprehensive and very large piece of legislation stand out? For present purposes, the provisions regarding the interception and monitoring of communications data need to be examined, as well as the so-called 'double-lock' process which is meant to be its main safeguard against abuses and a guarantor of due process.

2.1.1 The 'Double-Lock' process

The Bill will provide for an authorisation process under which warrants will be issued by the Secretary of State but will not come into force until approved by a Judicial Commissioner. This 'double-lock' process is much vaunted by the government as a fundamental safeguard to ensure that decisions to issue warrants must be subject to independent judges (called Judicial Commissioners in the Bill.) The double lock process will apply to warrants authorising, among others: interception of communication;[45] targeted equipment interference by the security and intelligence agencies and the Ministry of Defence;[46] bulk equipment interference;[47] the acquisition of communications data *in bulk*;[48] the obtaining, retaining and examination of bulk personal data by the security and intelligence agencies.[49]

The process is, at first glance, undeniably an improvement on previous uncertainty in that unilateral decisions are made impossible: The decision to issue a warrant must be taken personally by the Secretary of State, based on considerations including whether or not the warrant is necessary and proportionate. The decision then needs to be reviewed and approved by a Judicial

[43] The government published six draft codes of practice setting out how powers and obligations will work in practice. It is envisaged that the codes will be approved by Parliament and will have statutory force. They are the draft codes of practice on: National security notices (19 pages); Interception of communications (101 pages); Security and intelligence agencies' retention and use of bulk personal datasets (38 pages); Equipment interference (83 pages); Communications data (118 pages); and Bulk acquisition (50 pages).

[44] HANSARD, HOUSE OF COMMONS Vol. 607 col. 907 (March 15, 2016).

[45] Clause 19.

[46] Clause 90.

[47] Clause 138.

[48] Clauses 109 and 123.

[49] Clause 155.

Commissioner[50]according to the principles that would apply on judicial review. In this way the government proposes to guarantee that warrants are necessary, proportionate and lawful – i.e. by having a judge involved in assessing them as such. When warrants are to be renewed Judicial Commissioners are to provide the same safeguard.

The double-lock authorisation process was endorsed by the Committees that conducted pre-legislative scrutiny of the Bill.[51] And, in his extensive review of surveillance legislation, David Anderson QC recommended the executive as the primary authoriser with the judicial or independent authoriser controlling executive decisions by applying judicial review principles.[52] It is on this latter point that the double lock process may be criticized because, although in judicial review a judge reviews the lawfulness of a decision or action made by a public body, this is constrained to evaluating the form of the decision making process, rather than the substance of the decision. In other words, judicial reviews are a challenge to the way in which a decision has been made, rather than the rights and wrongs of the conclusion reached.[53] A strong case could be made for the argument that judicial oversight without the power to assess the substance of the government's decision amounts to very little oversight.

2.1.2 Retention of Communications data

The bill replicates broadly the existing statutory regimes by means of which telecoms operators can be required to retain communications, replacing ss1 and 2 of DRIPA and Part 11 of the Anti-Terrorism Crime and Security Act 2001.[54] It also largely replicates the effect of Chapter 2 of Part 1 of RIPA, providing public authorities with the power to acquire communications data, which will include the power to require the retention of Internet Connection Records (ICRs), which are classed as a form of communications data. This largely replicates the problems arising from the *Digital Rights Ireland* case[55] that DRIPA attempted to address, and in the light of the referral of the *Davis* case to the CJEU, [56]remains a problem until clarification is given by that Court.

2.1.3 Bulk data collection and retention

It has already been mentioned how the Snowden leaks revealed that the scope of GCHQ surveillance under TEMPORA,[57] stretched to the interception of millions of private communications and collection of bulk communications data.[58] Perhaps because of technological advances outracing the law, then extant legislation covering the intelligence services (such as the Security Service Act 1989 and the Intelligence Services Act 1994), through their silence on bulk data collection provided

---

[50] Judicial Commissioners will be former or serving High Court judges.

[51] HOME OFFICE, HUMAN RIGHTS MEMORANDUM 2016, *op. cit.,* para 27.

[52] DAVID ANDERSON QC, INDEPENDENT REVIEWER OF TERRORISM LEGISLATION, A QUESTION OF TRUST: REPORT OF THE INVESTIGATORY POWERS REVIEW, (Her Majesty's Stationery Office, June 2015), recommendations 84-88, 14.95.

[53] JUDICIARY OF THE UNITED KINGDOM, JUDICIAL REVIEW, (May 12, 2016), https://www.judiciary.gov.uk/you-and-the-judiciary/judicial-review/ accessed 15 May 2016.

[54] HOME OFFICE, HUMAN RIGHTS MEMORANDUM 2016, *op. cit.,* p.2.

[55] *See* 1.2.1 above.

[56] *See* 1.2.2 above.

[57] By using warrants for the interception of 'external communications' under section 8(4) RIPA.

[58] DSOU, 11.

loopholes for GCHQ to obtain bulk communications data, as well as private communications of millions of UK residents from foreign partners such as the NSA.[59]

With the IP Bill, the government's response to this seems to be not to condemn or close these loopholes but to give them legal sanction by explicitly building them into new legislation. For example, in its Section 19 statement in terms of the Human Rights Act 1998, the government comments on the Bill's proposed sanction of bulk personal data collection that, "[t]he security and intelligence agencies have existing statutory powers which enable them to acquire and use large datasets containing personal data. The Bill will not create a new power but will create safeguards…"[60] Professor Joseph Canatacci, the UN Special Rapporteur on Privacy (SRP) quite rightly stated that, '…disproportionate, privacy-intrusive measures such as bulk surveillance and bulk hacking as contemplated in the Investigatory Powers Bill [should] be outlawed rather than legitimised.'[61]

2.1.4 Secrecy requirement

In addition to any consideration about the IP Bill, its secrecy provisions, particularly sections 49 read with 50 should be kept in mind. These are draconian: Not only do they prohibit any information to be published or communicated about any surveillance, surveillance request, data request or warrant, they prohibit in absolute terms any revelation that such a request was made in the first place and they apply automatically to *any* warrant.

2.1.5 In summary:

The IP Bill is to be lauded for the 'double-lock' requirement that interception is overseen by judges who need to grant warrants, but it should not be overlooked that in turn, it hands law enforcement agencies more access to individuals' internet connection records than ever before: It requires web and phone companies to store records of websites visited by every citizen for 12 months for access by police, security services and other public bodies. For the first time ever it makes it legally explicit that security services have the power to collect in bulk large volumes of personal communications data, and security services and police have the power to hack into and bug computers and phones and what is more, a new legal obligation is placed on companies to assist in these operations to bypass encryption.[62] Recently in the US, the government backed down over forcing tech giant Apple to unlock a terrorist's iPhone – under the IP Bill, if the same scenario plays out in the UK, Apple would be under a legal obligation to comply with such a request.[63]

---

[59] DSOU, 11. See also the Government's Open Response to the claims brought by Liberty and Privacy International before the Investigatory Powers Tribunal in relation to Prism and Tempora, para 194.3.

[60] HOME OFFICE, HUMAN RIGHTS MEMORANDUM, 2016 p. 3 para 12.

[61] JOSEPH A. CANATACI, REPORT OF THE SPECIAL RAPPORTEUR ON THE RIGHT TO PRIVACY, (UN Human Rights Council, March 8, 2016) A/HRC/31/64, p 14.

[62] Alan Travis, *Investigatory powers bill: the key points*, *The Guardian*, (Nov 4, 2015), available at https://www.theguardian.com/world/2015/nov/04/investigatory-powers-bill-the-key-points (last accessed June 27, 2016).

[63] Devlin Barrett and Daisuke Wakabayashi, *FBI Opens San Bernardino Shooter's iPhone; U.S. Drops Demand on Apple – Move delays a high-stakes showdown between Washington, Silicon Valley, The Wall Street Journal*, (March 28, 2016), available at http://www.wsj.com/articles/fbi-unlocks-terrorists-iphone-without-apples-help-1459202353 (accessed 16 May 2016). See also Richard Yorke, *Silencing the Canary: the lawfulness of the U.K. Investigatory Powers Bill's secrecy provisions under the ECHR, EJIL: Talk!* Blog of the European Journal of

2.2 Arguments for and against the IP Bill

GCHQ and the Government backers of the Bill argue that bulk interception is necessary as a first step in the process of fighting terrorism and crime. Nobody disagrees that the sophisticated and unique modern iterations of both terrorism and organised crime necessitate a strong response.[64] The way in which this is done is of course contentious. GCHQ argues that the necessary second step is a targeted search of this data carried out under legal warrants and this means, according to them, that the vast majority of intercepted material is never read. A problem with this line of thinking is of course that even if the majority of data is indeed not read, the mere fact of authorising bulk interception legitimises mass surveillance.[65] Furthermore, as was pointed out earlier, data could be analysed to a remarkably precise degree without having to be read, as such.

The complex and controversial bill has, for this and other reasons, been the subject of fierce opposition and criticism, including two hundred leading lawyers representing the legal profession and forty UK law schools, as well as the United Nations Special Rapporteur on privacy.[66] A short scrutiny of changes suggested by the Labour party highlight some of the more obvious shortcomings of the Bill:

- "A clear definition of protecting 'national security' and 'economic wellbeing', which are the current conditions that justify the use of the new powers;
- A proportionate list of crimes that would justify allowing police and security services to access someone's internet connection record;
- Restrictions on the number of law enforcement agencies that would be allowed to use the legislation; Better protections for the confidential communications of 'sensitive professions' such as MPs with constitutents, lawyers with clients and journalists with sources;
- Approval for interception to be granted by judges on the basis of the evidence rather than merely whether the right process has been followed." 67

3. Cost-Benefit analysis

International Law (May 17, 2016), available at http://www.ejiltalk.org/silencing-the-canary-the-lawfulness-of-the-u-k-investigatory-powers-bills-secrecy-provisions-under-the-echr/ (accessed 17 May 2016).

[64] *See* the parliamentary debate around the second reading of the Bill, in which all participants accepted the need to update existing laws dealing with surveillance targeting terrorism and crime - HANSARD*,* HC (March 15,2016) Vol. 607 col. 810 – 907. For example: Labour's Andy Burnham said during the Bill's second debate that he was persuaded that the police and security services were losing the race against criminals because of advances in technology and that the law therefore needed to be updated to give a 'clear legal framework for access to some internet records. *See* also Rowena Mason, Anushka Asthana and Alan Travis, *'Snooper's charter': Theresa May faces calls to improve bill to protect privacy, The Guardian* (March 15, 2016), available at https://www.theguardian.com/world/2016/mar/15/delay-investigatory-powers-bill-scrutiny-mps-second-reading-firms-campaigners (last accessed June 27, 2016).

[65] CANNATACI, *op. cit.*, p 14. *See* also Owen Bowcott, Legal Affairs Correspondent, "Investigatory powers bill not fit for purpose, say 200 senior lawyers" *The Guardian* (March 14, 2016), available at https://www.theguardian.com/world/2016/mar/14/investigatory-powers-bill-not-fit-for-purpose-say-200-senior-lawyers (last accessed June 27, 2016).

[66] Ibid.

[67] *See* Rowena Mason, Anushka Asthana and Alan Travis, *op. cit.*(n. 64).

The focus now needs to turn to the third part of this analysis, judging the likelihood of the proposed legislative reform achieving its stated aims (such as prevention of terrorist atrocities) against its likely impacts, in this instance on freedom of expression in the UK.

3.1 Why protect Freedom of Expression?

Western philosophy recognised freedom of speech long before its inclusion in the 1948 Human Rights Declaration: Mill's classic essay 'Of the Liberty of Thought and Discussion', dating back to 1859, has proven to be an enduring starting point on the topic.[68] Today freedom of expression is one of the most highly valued human rights, with almost universal acceptance as a *sine qua non* for democratic societies. To name but a few: the Universal Declaration of Human Rights recognises this right in Article 19, the European Convention of Human Rights (ECHR) recognises it in Article 10 (Freedom of Expression)[69] and the Charter of Fundamental Rights of the European Union (the EU Charter) recognises in Article 11 the right to freedom of expression and information.[70] Free speech is therefore undeniably an established right. But every now and again, especially when faced with a situation where it may be affected, for example by proposed legislation such as the IP Bill, it is a good idea to take a step back and re-examine the reasons why it is deemed necessary to protect free speech. Only in such manner can the interests served by this right be judged against the interests served by the proposed infringing measure, and a proper balance sought.

Eric Barendt in his seminal work *Freedom of Speech* provides a clear and concise summary and analysis of the overarching reasons for protection this right.[71] In essence, there are four almost universally recognised arguments in favour of a Free Speech Principle: The argument concerning the importance of discovering truth; Free speech as an aspect of self-fulfilment; The argument from citizen participation in a democracy; and Suspicion of government. It is immediately evident that if freedom of expression is indeed impacted negatively by the IP Bill, all four arguments may be engaged. The four arguments feed into the protection of the following interests: The speaker's interest in communicating ideas and information; The audience's interest in receiving ideas and information; and the bystanders' (or public) interest in speech.[72] Of course the right to freedom of expression is not absolute and needs to be balanced against other values. For example, hate speech must be curbed in order to protect the right to human dignity. Nevertheless free speech is

---

[68] JOHN STUART MILL, ON LIBERTY (London: Longman, Roberts & Green, 1869, originally published 1859).

[69] Article 10 reads as follows: 1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This Article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises. 2. The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.

[70] Article 11 states: 1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. 2. The freedom and pluralism of the media shall be respected.

[71] ERIC BARENDT, FREEDOM OF SPEECH (2nd edn OUP, Oxford 2005), chapter 1 ('Why Protect Free Speech?'). See also on this topic DARIO MILO, DEFAMATION AND FREEDOM OF SPEECH (OUP, Oxford 2000), chapter 3 ('Freedom of Expression and Freedom of the Media) and in general, RONALD DWORKIN, FREEDOM'S LAW (OUP, New York 1996) and ANDRÁS KOLTAY, FREEDOM OF SPEECH: THE UNREACHABLE MIRAGE (Budapest: CompLex Publisher Ltd., 2013).

[72] *Ibid.*, 23-29.

important enough to be granted constitutional protection. In cases where free speech become constrained, we now commonly speak of the 'chilling effect'.

It is recognised that the State poses actual dangers with regard to freedom of speech, albeit in their modern iteration radically different from even a few decades ago. Koltay,[73] for instance, points out that the possibility of *direct* limitation of freedom of speech by the State is today severely restrained and circumscribed by constitutional guarantees and judicial precedent. However, indirect action by the State may nevertheless serve to constrain freedom of speech: To take but one example, deregulation of the media (or other areas of civic life), in effect transfers control of public discourse to powerful private interests, thus undermining the very raison d'être of a free and independent press to further a free and frank exchange of a variety of views. Similarly in our analysis the proposed legislation, once enacted and once its implications become clear to the public, may transform public discourse by skewing the free and frank exchange of ideas and information.

Wright rightly highlights the view that abuse of mass surveillance may be inimical to democracy as it erodes the trust between government and the governed and the civic sphere: 'There is no such thing as benign surveillance. It always comes with costs because of the chill it visits on conduct, education, associations, and expression'.[74] We therefore need to examine the chilling effect in terms of its effect on state action and its standing as a concept recognised in law in the UK and Europe.

3.2 Existing concern about chilling effect

3.2.1 The chilling effect in European Court of Human Rights jurisprudence

It has been noted that the ECtHR often remarks that certain measures and sanctions interfering with the right to freedom of expression have a "chilling effect".[75] Although mention of the chilling effect is not limited to freedom of expression jurisprudence under art.10, it arises in that context the most. Furthermore, it has been applied in relation to a variety of state interferences, including for example abortion laws,[76] and interferences with the right of individual petition under art.34.[77] One scholar reckoned that the phrase had been mentioned in over 100 judgments up to 2013, (so it is surprising that at the same time there has been a notable absence of scholarly attention to the judicial significance of this chilling effect principle.)[78]

In essence, the ECtHR jurisprudence seem to indicate that only a narrow margin should be allowed to a state when the restriction of free speech concerns political speech or is likely to discourage people from making criticisms or contributing to public discussion of issues affecting the life of the community.[79] Two remarks may be made here: A vote to leave the European Union does not affect, without more, the UK's relationship with the European Court of Human Rights and its jurisprudence

---

[73] KOLTAY, *op cit.,*92-96.

[74] *See* ANDREW MCCANSE WRIGHT, CIVIL SOCIETY AND CYBERSURVEILLANCE (June 24, 2016), 1, 3. Available at SSRN: http://ssrn.com/abstract=2800200.

[75] *See* Ronan O Fathaigh, *Article 10 and the chilling effect principle* E.H.R.L.R. 304 (2013).

[76] *See* e.g. *Tysiaç v Poland* 45 E.H.R.R. 42 (2007) at [116]; and *A v Ireland* 53 E.H.R.R. 13 (2011) at [178].

[77] *See* e.g. *McShane v United Kingdom* 35 E.H.R.R. 23 (2002)at [151], and *Colibaba v Moldova* 49 E.H.R.R. 44 (2009)at [68].

[78] O Fathaigh, *op. cit.,* 304.

[79] *See*, especially, the judgement in *Lingens v Austria* 8 EHRR 407 (1986) and Valia Filipova, *Standards of Protection of Freedom of Expression and the Margin of Appreciation in the Jurisprudence of the European Court of Human Rights* Cov. L.J. 64 (2012).

and therefore until such time as (and if) the UK ends this relationship, the ECHR and the decisions by the ECtHR will continue to play an important part in domestic jurisprudence. Secondly, the ECtHR's jurisprudence relevant to the IP Bill's likely impact on freedom of expression unfortunately seems to have fallen by the wayside – at least as far as the discussion of the proposed legislation is concerned. Anecdotally, for instance, the author counted in the May 2016 Parliamentary debate of the IP Bill,[80] more than a hundred mentions of the word 'privacy' by MPs representing the full range of British political parties whereas in the same debate 'freedom of speech' was mentioned twice, and 'freedom of expression' once only.[81]

Furthermore, the ECtHR has also clearly ruled in *Vereniging Weekblad Bluf! V Netherlands* that legislation that prohibits the dissemination of national security information which eliminates public control over intelligence services' activities, in absolute and unconditional terms, constitutes a breach of art. 10 as it goes beyond what is necessary in a democratic society.[82] It could be argued that requiring telecoms operators to retain and hand over to the government bulk data, combined with the secrecy requirement fall foul of the *Vereniging Weekblad Bluf!* ruling.

3.2.2 The chilling effect in the UK

Activists have long pointed out that the United Kingdom needs to be concerned about its protection of the right to free speech: For some time these concerns have been centred round the UK's libel law which was perceived to stifle free and frank exchange of ideas. The European Parliament, for example, in May 2012 termed the defamation regime in England and Wales 'the most claimant-friendly in the world'.[83] As such it was argued to have a chilling effect on freedom of expression, in that the mere threat of a libel action could serve as a deterrent to speech. Since such a chilling effect is in reality a form of self-censorship, it is particularly difficult to gauge. Nevertheless, the chilling effect was considered real enough to prompt the wholesale reform of English defamation law, which culminated in the Defamation Act 2013.

It would be ironic if one area of the law is substantially reformed to encourage freedom of speech whilst shortly afterward another legal regime is established that possibly (hopefully) unintentionally reintroduces the chilling effect. The Home Office acknowledges '…the possibility of interception has the ability to discourage freedom of expression and public discourse and therefore interfere with Article 10 rights' but in contrast to its extensive response to privacy concerns raised by campaigners, say little about how Article 10 infringement will be countered.[84]

Conclusion

On the one hand we have legislation that aims to prevent major acts of terrorism partly by curtailing civil rights such as freedom of expression. But how do we judge whether this will work? Can the (so far since the London attacks of 2005 and hopefully continued) absence of major terrorist atrocities in the UK on the scale recently witnessed in Europe and the Middle East be seen as proof of the efficacy of covert and overt surveillance? These operations are by their nature veiled in secrecy – and if they have so far succeeded in preventing crime or terrorist activity, the government is keeping

---

[80] *Op. cit.,* n 44.

[81] Scott Mann (Conservative) at col. 885 and Rob Marris (Labour) at col. 916.

[82] *Vereniging Weekblad Bluf! V. the Netherlands* (A/306-A) ECtHR 20 E.H.R.R. 189 (1995).

[83] European Parliament Resolution of 10 May 2012 (2013/C 261 E/03), paras C-E.

[84] HOME OFFICE, HUMAN RIGHTS MEMORANDUM 2016, *op. cit.,* at 7.

quiet. Anecdotally, it would seem that most of the possible terrorist attacks planned in the UK were prevented through means other than intrusive surveillance: informants, old fashioned boots on the ground police work, and blind luck seem to have been the main bulwarks in this area.[85] On the other hand we have a right, the exercise of which is difficult if not impossible to gauge. It is difficult to measure whether free speech is or has been chilled - and even more so to predict the likely effect in future. What is certain, and had been convincingly argued before, is that the impact of mass surveillance could potentially affect the exercise of expressive freedoms to such an extent that it may pose a threat to the very idea of democracy itself.[86]

Thomas Jefferson's famous sentiment was that freedom of expression 'cannot be limited without being lost.'[87] Yet experience has shown that absolute freedom of expression either is not workable or comes at (perhaps) too high a price. It already seems as if it is inevitable that in modern life a large degree of individual privacy must be sacrificed on the altar of public security. Will the same fate befall public and private discourse? In effect, what the government seems to be presenting us with is a double bind; the choice between two evils, and its answer with the IP Bill seems to be that less freedom of expression, measured against safety, security and crime, is the lesser of two evils. This is a presumption that cannot be allowed to go unchallenged. The author hopes that at least the same consideration and thought currently being devoted to privacy concerns will be accorded to free speech, before the IP Bill becomes law.

The following sentiment perhaps puts it best:

> "History … teaches us that ideals (this time the ideal of freedom of speech) that we long for so much have (and could never and nowhere) been realised in full. *Freedom of speech is an ideal, an unattainable mirage* which, as we try to approach it, first loses its contours, then becomes blurry and finally dissipates without a trace in the hot summer air. However, it does not entitle us to quit making increasingly desperate efforts to get closer to it anyway."[88]

[85] For just a few examples of terrorist plots foiled by luck, chance, police work, etc., *see* Marco Giannangelli, *ISIS plot on London, Brighton, Bath and Ipswich FOILED as pilots discuss targets on radio, Express Online* (Jan 25, 2016), available at http://www.express.co.uk/news/uk/637451/RAF-foils-airline-terror-plot-four-British-cities-pop-song-code (last accessed Jun 27, 2016) and Danny Shaw, *Terrorism plot size of 7/7 attacks 'foiled every year', BBC*, (March 21, 2013) available at http://www.bbc.co.uk/news/uk-21878867 (last accessed Jun 27, 2016).

[86] *See* Ronald J. Krotoszynski, Jr., *Reconciling Privacy and Speech in the Era of Big Data: A Comparative Legal Analysis*, 56 WM. & MARY L. REV. 1279, 1287 (2015).

[87] Letter to James Currie, 28 January 1786, Library of Congress.

[88] KOLTAY, *op. cit.,*96.